

A NOTE ON THE NO-THREE-IN-LINE PROBLEM ON A TORUS

ALEKSANDER MISIAK, ZOFIA STĘPIEŃ, ALICJA SZYMASZKIEWICZ,
LUCJAN SZYMASZKIEWICZ, AND MACIEJ ZWIERZCHOWSKI

ABSTRACT. In this paper we show that at most $2\gcd(m, n)$ points can be placed with no three in a line on an $m \times n$ discrete torus. In the situation when $\gcd(m, n)$ is a prime, we completely solve the problem.

1. INTRODUCTION

The no-three-in-line-problem [2] asks for the maximum number of points that can be placed in the $n \times n$ grid with no three points collinear. This question has been widely studied, but is still not resolved.

The obvious upper bound is $2n$ since one can put at most two points in each row. This bound is attained for many small cases, for details see [4] and [5]. In [7] the authors give a probabilistic argument to support the conjecture that for a large n this limit is unattainable.

As a lower bound, Erdős' construction (see [3]) shows that for p prime one can select p points with no three collinear. In [8] it is shown, that for p prime one can select $3(p-1)$ points from a $2p \times 2p$ grid with no three collinear.

In the literature we can find some extensions of the no-three-in-line problem (see [6], [9]). This paper is generalization of [6], where authors analyze the no-three-in-line-problem on the discrete torus. This modified problem is still interesting.

Let m and n be positive integers greater than 1. By a discrete torus $T_{m \times n}$ we mean $\{0, 1, \dots, m-1\} \times \{0, 1, \dots, n-1\}$.

Four integers a, b, u, v with $\gcd(u, v) = 1$ correspond to the line $\{(a + uk, b + vk) : k \in \mathbb{Z}\}$ on $\mathbb{Z} \times \mathbb{Z}$. The condition $\gcd(u, v) = 1$ ensures that each pair P, Q of distinct points in $\mathbb{Z} \times \mathbb{Z}$ belongs to exactly one line. For instance, the points $O = (0, 0)$, $P = (2, 2)$ belong to the line $\{(k, k) : k \in \mathbb{Z}\}$.

We define lines on $T_{m \times n}$ to be images of lines in the $\mathbb{Z} \times \mathbb{Z}$ under the projection $\pi_{m,n} : \mathbb{Z} \times \mathbb{Z} \rightarrow T_{m \times n}$ defined as follows

$$\pi_{m,n}(a, b) := (a \bmod m, b \bmod n).$$

By $x \bmod y$ we mean the smallest non-negative remainder when x is divided by y .

We say that a set $X \subset T_{m \times n}$ satisfies the no-three-in-line condition if there are no three collinear points in X . Let $\tau(T_{m \times n})$ denote the size of the largest set X satisfying the no-three-in-line condition.

In our paper we will prove the following theorems.

Theorem 1.1. *We have*

$$\tau(T_{m \times n}) \leq 2\gcd(m, n).$$

Theorem 1.2. *We have*

2000 *Mathematics Subject Classification.* 05B99.

Key words and phrases. Discrete torus; No-three-in-line problem; Chinese Remainder Theorem.

Corresponding author: Z. Stępień; e-mail: stepien@zut.edu.pl; Tel/fax: +48914494826.

- (1) For $\gcd(m, n) = 1$, $\tau(T_{m \times n}) = 2$.
- (2) For $\gcd(m, n) = 2$, $\tau(T_{m \times n}) = 4$.
- (3) Let $\gcd(m, n) = p$ be an odd prime.
 - (a) If $\gcd(pm, n) = p^2$ or $\gcd(m, pn) = p^2$, then $\tau(T_{m \times n}) = 2p$.
 - (b) If $\gcd(pm, n) = p$ and $\gcd(m, pn) = p$, then $\tau(T_{m \times n}) = p + 1$.

The Theorem 1.2(1) was proved in [6] by some algebraic argument. The Theorem 1.2(2) is a generalized version of Proposition 2.1 from [6]. Similarly, Theorem 1.2(3a) and Theorem 1.2(3b) are generalizations of Theorem 2.7 and Theorem 2.9 from [6], respectively.

2. PROOFS OF THEOREM 1.1 AND THEOREM 1.2(1)

One of the main tools used in this paper is the Chinese Remainder Theorem.

Theorem 2.1 (Chinese Remainder Theorem). *Two simultaneous congruences*

$$\begin{aligned} x &\equiv a \pmod{m}, \\ x &\equiv b \pmod{n} \end{aligned}$$

are solvable if and only if $a \equiv b \pmod{\gcd(m, n)}$. Moreover, the solution is unique modulo $\text{lcm}(m, n)$.

Let us define the family $\mathcal{L} = \{L_s : s \in \{0, 1, \dots, \gcd(m, n) - 1\}\}$ of lines on $T_{m \times n}$, where

$$L_s = \{\pi_{m,n}(k, k - s) \in T_{m \times n} : k \in \mathbb{Z}\}.$$

Lemma 2.2 (see [10]). *Let $a = (a_x, a_y) \in T_{m \times n}$ and $d = (a_x - a_y) \bmod \gcd(m, n)$. Then $a \in L_d$. Moreover, we have $L_{s_1} \cap L_{s_2} = \emptyset$ for $s_1 \neq s_2$ and $s_1, s_2 \in \{0, 1, \dots, \gcd(m, n) - 1\}$.*

Proof. By Theorem 2.1 there exists $k \in \mathbb{Z}$ such that

$$\begin{aligned} k &\equiv a_x \pmod{m}, \\ k &\equiv a_y + d \pmod{n}. \end{aligned}$$

Consequently, $(a_x, a_y) = \pi_{m,n}(k, k - d) \in L_d$. Suppose that $L_{s_1} \cap L_{s_2} \neq \emptyset$. This means that there are $k_1, k_2 \in \mathbb{Z}$ such that $\pi_{m,n}(k_1, k_1 - s_1) = \pi_{m,n}(k_2, k_2 - s_2)$. In other words $k_1 - k_2$ is the solution of the following system

$$\begin{aligned} k_1 - k_2 &\equiv 0 \pmod{m}, \\ k_1 - k_2 &\equiv s_1 - s_2 \pmod{n}. \end{aligned}$$

By Theorem 2.1 again, we see that $s_1 - s_2 \equiv 0 \pmod{\gcd(m, n)}$. Hence $L_{s_1} \cap L_{s_2} = \emptyset$ for $s_1 \neq s_2$ and $s_1, s_2 \in \{0, 1, \dots, \gcd(m, n) - 1\}$. \square

Proof of Theorem 1.1. Let $X \subset T_{m \times n}$ satisfy the no-three-in-line condition. By Lemma 2.2 for every $a \in X$ there exists $L \in \mathcal{L}$ such that $a \in L$. Consequently, $\tau(T_{m \times n}) \leq 2 \cdot |\mathcal{L}| = 2 \cdot \gcd(m, n)$. \square

Proof of Theorem 1.2(1). Obviously it is always true that $\tau(T_{m \times n}) \geq 2$. By Theorem 1.1 we get the statement. \square

3. PROOFS OF THEOREM 1.2(2) AND THEOREM 1.2(3A)

Let $X = (x_1, x_2) \in \mathbb{Z} \times \mathbb{Z}$, $Y = (y_1, y_2) \in \mathbb{Z} \times \mathbb{Z}$, $Z = (z_1, z_2) \in \mathbb{Z} \times \mathbb{Z}$. Denote by $D(X, Y, Z)$ the following determinant

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix}$$

Recall the determinant criterion for checking whether points are in a line:

Lemma 3.1. *Three points $X, Y, Z \in \mathbb{Z} \times \mathbb{Z}$ are in a line if and only if $D(X, Y, Z) = 0$.*

Now we prove the determinant criterion on a torus.

Lemma 3.2. *If three points a, b and c of $T_{m \times n}$ are in a line, then $D(a, b, c) \equiv 0 \pmod{\gcd(m, n)}$.*

Proof. Suppose that three points $a = (a_x, a_y)$, $b = (b_x, b_y)$ and $c = (c_x, c_y)$ are in a line on $T_{m \times n}$. This means that there are $A, B, C \in \mathbb{Z} \times \mathbb{Z}$ such that $\pi(A) = a$, $\pi(B) = b$, $\pi(C) = c$ and $D(A, B, C) = 0$. More precisely

$$\begin{aligned} A &= (a_x + \alpha_x m, a_y + \alpha_y n), \\ B &= (b_x + \beta_x m, b_y + \beta_y n), \\ C &= (c_x + \gamma_x m, c_y + \gamma_y n) \end{aligned}$$

for some $\alpha_x, \alpha_y, \beta_x, \beta_y, \gamma_x, \gamma_y \in \mathbb{Z}$.

We get

$$\begin{aligned} 0 &= D(A, B, C) = D(a, b, c) + nD((a_x, \alpha_x), (b_x, \beta_y), (c_x, \gamma_y)) \\ &\quad + mD((\alpha_x, a_y), (\beta_x, b_y), (\gamma_x, c_y)) + mnD((\alpha_x, \alpha_y), (\beta_x, \beta_y), (\gamma_x, \gamma_y)). \end{aligned}$$

Hence $D(a, b, c) \equiv 0 \pmod{\gcd(m, n)}$. \square

Proof of Theorem 1.2(2). Let $\gcd(m, n) = 2$. Let

$$X = \{(0, 0), (0, 1), (1, 0), (1, 1)\} \subset T_{m \times n}.$$

It is easy to check that $D(a, b, c) \equiv \pm 1 \pmod{\gcd(m, n)}$ for any $a, b, c \in X$. By Lemma 3.2, X satisfies the no-three-in-line condition. Thus $\tau(T_{m \times n}) \geq 4$. Now Theorem 1.1 finishes the statement. \square

Proof of Theorem 1.2(3a). Let $p = \gcd(m, n)$ be an odd prime. Assume without loss of generality that $\gcd(pm, n) = p^2$. Consequently $m = pk$ and $n = p^2l$ for some positive integers k, l . Define $X = \{(i, i^2p) \in T_{m \times n} : i \in \{0, 1, \dots, p-1\}\}$ and $Y = \{(i, i^2p+1) \in T_{m \times n} : i \in \{0, 1, \dots, p-1\}\}$. We will show that the set $X \cup Y$ of $2p$ points satisfies the no-three-in-line condition.

Take any three distinct points $(i, i^2p), (j, j^2p), (k, k^2p)$ from X . We will show that these points are not in a line on $T_{m \times n}$. To do this, we will show that three points $A = (i + \alpha_x m, i^2p + \alpha_y n)$, $B = (j + \beta_x m, j^2p + \beta_y n)$, $C = (k + \gamma_x m, k^2p + \gamma_y n)$, where $\alpha_x, \alpha_y, \beta_x, \beta_y, \gamma_x, \gamma_y \in \mathbb{Z}$ are not in a line on $\mathbb{Z} \times \mathbb{Z}$. We get

$$\begin{aligned} D(A, B, C) &= D((i, i^2p), (j, j^2p), (k, k^2p)) + nD((i, \alpha_y), (j, \beta_y), (k, \gamma_y)) \\ &\quad + mD((\alpha_x, i^2p), (\beta_x, j^2p), (\gamma_x, k^2p)) + mnD((\alpha_x, \alpha_y), (\beta_x, \beta_y), (\gamma_x, \gamma_y)) \\ &= p \cdot D((i, i^2), (j, j^2), (k, k^2)) + p^2l \cdot D((i, \alpha_y), (j, \beta_y), (k, \gamma_y)) \\ &\quad + pk \cdot p \cdot D((\alpha_x, i^2), (\beta_x, j^2), (\gamma_x, k^2)) + pk \cdot p^2l \cdot D((\alpha_x, \alpha_y), (\beta_x, \beta_y), (\gamma_x, \gamma_y)) \\ &= p(j-i)(k-i)(k-j) + p^2M \neq 0, \end{aligned}$$

since $p \nmid (j-i)(k-i)(k-j)$ and $M \in \mathbb{Z}$.

In the same way it can be shown that any three points from Y are not in a line on $T_{m \times n}$.

Now take any two points $(i, i^2p), (j, j^2p)$ from X and (k, k^2p+1) from Y . We have

$$D((i, i^2p), (j, j^2p), (k, k^2p+1)) \equiv j-i \pmod{\gcd(m, n)}.$$

By Lemma 3.2 these points are not in a line. The same argument works if we take one point from X and any two points from Y . We showed that $\tau(T_{m \times n}) \geq 2p$. Now Theorem 1.1 gives the statement. \square

4. PROOF OF THEOREM 1.2(3B)

Let $p = \gcd(m, n)$ and $\rho : T_{m \times n} \rightarrow T_{p \times p}$ be the projection defined as follows $\rho(u, v) = (u \bmod p, v \bmod p)$. Since $p|m$ and $p|n$, the diagram

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{\pi_{m,n}} & T_{m \times n} \\ \pi_{p,p} \downarrow & \swarrow \rho & \\ T_{p \times p} & & \end{array} \quad (1)$$

commutes. Consequently, the image of every line on $T_{m \times n}$ is a line on $T_{p \times p}$. This immediately implies the following result.

Lemma 4.1. *Let $p = \gcd(m, n)$. The following holds:*

- (1) $\tau(T_{m \times n}) \geq \tau(T_{p \times p})$,
- (2) *If the preimage of every line on $T_{p \times p}$ is a line on $T_{m \times n}$, then $\tau(T_{m \times n}) = \tau(T_{p \times p})$.*

Now, let us define the family $\mathcal{P}_O = \{\ell^\beta : \beta \in \{0, 1, \dots, p-1\}\} \cup \{\ell^\infty\}$ of lines on $T_{p \times p}$ passing through $O = (0, 0)$, where

$$\begin{aligned} \ell^\beta &= \{\pi_{p,p}(k, \beta k) \in T_{p \times p} : k \in \mathbb{Z}\}, \\ \ell^\infty &= \{\pi_{p,p}(0, k) \in T_{p \times p} : k \in \mathbb{Z}\}. \end{aligned}$$

The following results can also be found in [6].

Lemma 4.2. *Let p be an odd prime. Then $T_{p \times p} = \bigcup_{\ell \in \mathcal{P}_O} \ell$.*

Proof. Consider $(a_x, a_y) \in T_{p \times p}$. Suppose $a_x \neq 0$. Since p is an odd prime, there is a unique $\beta \in \{0, 1, \dots, p-1\}$ such that $(a_x, a_y) \in \ell^\beta$. If a_x is zero, then $(a_x, a_y) \in \ell^\infty$. Hence, $T_{p \times p} \subset \bigcup_{\ell \in \mathcal{P}_O} \ell$. The inclusion $\bigcup_{\ell \in \mathcal{P}_O} \ell \subset T_{p \times p}$ is obvious. \square

In the next two lemmas we will investigate the sets $\rho^{-1}(\ell)$ for $\ell \in \mathcal{P}_O$.

Lemma 4.3. *Let p be an odd prime. For every $\beta \in \{1, 2, \dots, p-1\}$ the set $\rho^{-1}(\ell^\beta)$ is a line on $T_{m \times n}$.*

Proof. First we claim that there is $\alpha \in \mathbb{Z}$ such that $\alpha \equiv \beta \pmod{p}$ and $\gcd(\alpha m, n) = p$. Indeed, for instance, take α such that the following conditions are satisfied: (i) $\alpha = \beta + kp$ for some $k \in \mathbb{Z}$, (ii) α is a prime, (iii) α is greater than n . Since p is an odd prime, the existence of such α is guaranteed by Dirichlet's theorem on arithmetic progressions.

Define $L^\alpha = \{\pi_{m,n}(k, \alpha k) : k \in \mathbb{Z}\}$. Now, we will show that $\rho^{-1}(\ell^\beta) = L^\alpha$. Let $(a_x, a_y) \in \rho^{-1}(\ell^\beta)$. Then $a_y \equiv \beta a_x \pmod{p}$ and $a_y \equiv \alpha a_x \pmod{p}$. By Theorem 2.1 there exists $k_1 \in \mathbb{Z}$ such that

$$\begin{aligned} k_1 &\equiv \alpha a_x \pmod{\alpha m}, \\ k_1 &\equiv a_y \pmod{n}. \end{aligned}$$

It is easy to see that $k_1 = \alpha k$ for $k \in \mathbb{Z}$ and we get

$$\begin{aligned} \alpha k &\equiv \alpha a_x \pmod{\alpha m}, \\ \alpha k &\equiv a_y \pmod{n}. \end{aligned}$$

Hence

$$\begin{aligned} k &\equiv a_x \pmod{m}, \\ \alpha k &\equiv a_y \pmod{n}. \end{aligned}$$

This means that $(a_x, a_y) \in L^\alpha$. Since $\rho(L^\alpha) \subset \ell^\beta = \rho^{-1}(\ell^\beta)$, we have $L^\alpha \subset \rho^{-1}(\ell^\beta)$. The proof is finished.

□

Lemma 4.4. *Let $p = \gcd(m, n)$. The following holds:*

- (1) *If $\gcd(m, pn) = p$, then $\rho^{-1}(\ell^\infty)$ is a line in $T_{m \times n}$,*
- (2) *If $\gcd(pm, n) = p$, then $\rho^{-1}(\ell^0)$ is a line in $T_{m \times n}$.*

Proof. (1) Let $L^\infty = \{\pi_{m,n}(pk, k) : k \in \mathbb{Z}\}$. We will show that $\rho^{-1}(\ell^\infty) = L^\infty$. Take $(a_x, a_y) \in \rho^{-1}(\ell^\infty)$. Hence $a_x \equiv 0 \pmod{p}$. By Theorem 2.1 there exists $k_1 \in \mathbb{Z}$ such that

$$\begin{aligned} k_1 &\equiv a_x \pmod{m}, \\ k_1 &\equiv pa_y \pmod{pn}. \end{aligned}$$

It is easy to see that $k_1 = pk$ for some $k \in \mathbb{Z}$ and we get

$$\begin{aligned} pk &\equiv a_x \pmod{m}, \\ pk &\equiv pa_y \pmod{pn}. \end{aligned}$$

Hence

$$\begin{aligned} pk &\equiv a_x \pmod{m}, \\ k &\equiv a_y \pmod{n} \end{aligned}$$

and $a \in L^\infty$. The inclusion $L^\infty \subset \rho^{-1}(\ell^\infty)$ is obvious. The proof is finished.

(2) The proof is similar to (1). □

Theorem 4.5. *Let $p = \gcd(m, n)$ be an odd prime such that $\gcd(pm, n) = \gcd(m, pn) = p$. Then we have $\tau(T_{m \times n}) = \tau(T_{p \times p})$.*

Proof. By Lemma 4.4 and 4.3 we get that $\rho^{-1}(\ell)$ is a line on $T_{m \times n}$ for any $\ell \in \mathcal{P}_O$. Hence the preimage of every line on $T_{p \times p}$ is a line on $T_{m \times n}$. Lemma 4.1(2) finishes the proof. □

The following result can be found in [6]. Here we present the complete proof.

Theorem 4.6. *Let p be an odd prime. Then $\tau(T_{p \times p}) = p + 1$.*

Proof. Let p be an odd prime number. If $p \equiv 1 \pmod{4}$ then take q to be some quadratic nonresidue modulo p . If $p \equiv 3 \pmod{4}$ take q to be some quadratic residue modulo p . Define $X = \{(x, y) \in T_{p \times p} : x^2 + q \cdot y^2 \equiv 1 \pmod{p}\}$. It is known that X has $p + 1$ points. See for example Theorem 10.5.1 in [1]. By Lagrange theorem for congruences, any line intersects X in at most two points. Hence the set X satisfies the no-three-in-line condition and $\tau(T_{p \times p}) \geq p + 1$.

Let X satisfy the no-three-in-line condition. We can assume that $O \in X$. By Lemma 4.2, every other point of the $T_{p \times p}$ lies on one or the other of the $p + 1$ lines passing through O . Hence $|X| \leq p + 2$ and we have $\tau(T_{p \times p}) \leq p + 2$.

Assume that there exists a set Y with $p + 2$ points which satisfies the no-three-in-line condition. Take any line L in $T_{p \times p}$. We claim that either $|L \cap Y| = 0$ or $|L \cap Y| = 2$. Indeed, if $L \cap Y = \{y\}$ then L is the line passing through point $y \in Y$ which does not pass by any other point of Y and consequently $|Y| \leq p + 1$, a contradiction. Now fix any point z not in Y . Since each line through z contains either 0 or 2 points of Y , the number of points in Y is even, a contradiction with the fact that $p + 2$ is odd. This means that the set Y does not exist. □

Proof of Theorem 1.2(3b).

Theorem 4.5 together with Theorem 4.6 gives the statement. □

Acknowledgment. We express our sincere thanks to the anonymous referee for his/her valuable advice which resulted in an improvement of this article.

REFERENCES

- [1] B. C. Berndt, R. J. Evans, K. S. Williams, Gauss and Jacobi sums, Wiley, 1998.
- [2] H. E. Dudeney, Amusements in Mathematics, Nelson, Edinburgh 1917, pp. 94, 222.
- [3] P. Erdős. Appendix, in K.F. Roth, On a problem of Heilbronn, J. London Math. Soc. 26, 198–204, 1951.
- [4] A. Flammenkamp, Progress in the no-three-in-line problem, J. Combin. Theory Ser. A, 60(2), 305–311, 1992.
- [5] A. Flammenkamp, Progress in the no-three-in-line problem II, J. Combin. Theory Ser. A, 81(1), 108–113, 1998.
- [6] J. Fowler, A. Groot, D. Pandya, B. Snapp, The no-three-in-line problem on a torus, arXiv:1203.6604v1.
- [7] R. K. Guy P. A. Kelly, The No-Three-Line Problem, Math. Bull. Vol. 11, pp. 527–531, 1968.
- [8] R. R. Hall, T. H. Jackson, A. Sudbery, and K. Wild, Some advances in the no-three-in-line problem, J. Combinatorial Theory Ser. A, 18:336–341, 1975.
- [9] A. Por, D.R. Wood, No-Three-in-Line-in-3D, Algorithmica 47(4), 481–488, 2007.
- [10] Z. Stępień, L. Szymaszkiewicz, M. Zwierchowski, The Cartesian product of cycles with small 2-rainbow domination number, Journal of Combinatorial Optimization, doi:10.1007/s10878-013-9658-0.

SCHOOL OF MATHEMATICS, WEST POMERANIAN UNIVERSITY OF TECHNOLOGY, AL. PIASTÓW
48/49, 70-310 SZCZECIN, POLAND
E-mail address: Aleksander.Misiak@zut.edu.pl

SCHOOL OF MATHEMATICS, WEST POMERANIAN UNIVERSITY OF TECHNOLOGY, AL. PIASTÓW
48/49, 70-310 SZCZECIN, POLAND
E-mail address: stepien@zut.edu.pl

SCHOOL OF MATHEMATICS, WEST POMERANIAN UNIVERSITY OF TECHNOLOGY, AL. PIASTÓW
48/49, 70-310 SZCZECIN, POLAND
E-mail address: alicjasz@zut.edu.pl

INSTITUTE OF MATHEMATICS, SZCZECIN UNIVERSITY, WIELKOPOLSKA 15, 70-451 SZCZECIN,
POLAND
E-mail address: lucjansz@wmf.univ.szczecin.pl

SCHOOL OF MATHEMATICS, WEST POMERANIAN UNIVERSITY OF TECHNOLOGY, AL. PIASTÓW
48/49, 70-310 SZCZECIN, POLAND
E-mail address: mzwierz@zut.edu.pl